



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,686	01/24/2002	Niels Rump	SCHO0093	3745

7590 06/01/2006

GLENN PATENT GROUP  
3475 Edison Way  
Suite L  
Menlo Park, CA 94025

EXAMINER
----------

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 06/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/913,686

Applicant(s)

RUMP ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 03 March 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

1 This action is in response to the communication filed on 3/3/2006.

2 **DETAILED ACTION**

3 ***Continued Examination Under 37 CFR 1.114***

4 A request for continued examination under 37 CFR 1.114, including the fee set forth in  
5 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is  
6 eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)  
7 has been timely paid, the finality of the previous Office action has been withdrawn pursuant to  
8 37 CFR 1.114. Applicant's submission filed on 3/3/2006 has been entered.

9 ***Response to Arguments***

10 Applicant's arguments filed 8/17/2005 have been fully considered but they are moot in  
11 view of the new grounds of rejection presented below.

12 Claims 1-30 have been examined and claim 31 has been cancelled.

13 All objections and rejections not set forth below have been withdrawn.

14 ***Claim Rejections - 35 USC § 103***

15 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all  
16 obviousness rejections set forth in this Office action:

17 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in  
18 section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are  
19 such that the subject matter as a whole would have been obvious at the time the invention was made to a person  
20 having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the  
21 manner in which the invention was made.

22  
23 Claims 1-7, 14, 16-17, 19, 23, 25-29 are rejected under 35 U.S.C. 103(a) as being  
24 unpatentable over Van Oorschot et al. (US Patent Number 5,850,443) hereinafter referred to as  
25 Van Oorschot, and further in view of Nardone et al. (US Patent Number 5,805,700) hereinafter  
26 referred to as Nardone.

1           Regarding claim 1, Van Oorschot disclosed a method for producing a payload data  
2 stream comprising a header and a payload data block containing encrypted payload data (See  
3 Van Oorschot Fig. 3 X-fields, header fields, and encrypted message field), comprising the  
4 following steps: generating a payload data key for a payload data encryption algorithm for  
5 encrypting payload data (See Van Oorschot Col. 6 Lines 41-43 and Fig. 3 “Create low trust  
6 symmetric key” K’); encrypting a first section of the payload data using said payload data key  
7 and said payload data encryption algorithm to obtain an encrypted section of said payload data  
8 block of said payload data stream (See Van Oorschot Col. 6 Lines 42-43 and Fig. 3 “Symmetric  
9 encryption” and “encrypted message”), said first section including audio data, video data, a  
10 combination of audio data and video data, text data, or binary data forming an executable  
11 program (See Van Oorschot Abstract ciphertext), wherein a second section of the payload data  
12 remains unencrypted (See Van Oorschot Col. 6 Lines 45-47 “public key of entity A”);  
13 processing the unencrypted section of said payload data (See Van Oorschot Col. 6 Lines 45-50  
14 “hash of X” which contains the public key of A) to deduce information characterizing the  
15 unencrypted second section of said payload data (See Van Oorschot Col. 6 Lines 49-60  $h40(X)$ );  
16 linking said information and said payload data key by means of an invertible logic linkage to  
17 obtain a basic value (See Van Oorschot Col. 6 Lines 56-60 “K’ XOR  $h40(X)$ ”); encrypting said  
18 basic value using a key of two keys being different from each other by an asymmetrical  
19 encryption method, said two different keys being the public and the private keys respectively for  
20 said asymmetrical encryption method, to obtain an output value being an encrypted version of  
21 said payload data key (See Van Oorschot Col. 6 Line 60 – Col. 7 Line 7); and entering said  
22 output value into said header of said payload data stream (See Van Oorschot Col. 6 Line 65 –

Art Unit: 2131

1 Col. 7 Line 7 and Fig. 3 “A’s header field” and “B’s header field”), but Van Oorschot failed to  
2 disclose that the second section included audio data, video data, a combination of audio data and  
3 video data, text data, or binary data forming an executable program.

4 Nardone teaches that movie data needs to be protected from being copied and that this is  
5 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further  
6 that in order to save on processing cost, only portions of the movie data should be encrypted (See  
7 Nardone Col. 1 Summary of the Invention).

8 It would have been obvious to the ordinary person skilled in the art at the time of  
9 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by  
10 encrypting video data, and further by only encrypting portions of the data. This would have been  
11 obvious because the ordinary person skilled in the art would have been motivated to protect  
12 movie data and to save on processing cost.

13 Regarding claim 17, Van Oorschot disclosed a method for decrypting an encrypted  
14 payload data stream comprising a header and a payload data block containing a first section  
15 having encrypted payload data (encrypted message), said first section including audio data, video  
16 data, a combination of audio data and video data, text data, or binary data forming an executable  
17 program (See Van Oorschot Abstract ciphertext), and a second section having unencrypted  
18 payload data (public key of A), said header comprising an output value having been generated by  
19 an encryption of a basic value by an asymmetrical encryption method using a key of two  
20 different keys including a private and a public key, said basic value representing a linkage of a  
21 payload data key, with which said first section having encrypted payload data is encrypted using  
22 a payload data encryption algorithm, and information deduced by a certain processing of the

1 unencrypted second section of the payload data, said information characterizing a certain part of  
2 said payload data stream unambiguously (See rejection of claim 1 above), said method  
3 comprising the following steps: obtaining said output value from said header (See Van Oorschot  
4 Fig. 4 “B’s Header Field” and Col. 4 Lines 51-52); decrypting said output value using the other  
5 key of said asymmetrical encryption method to obtain said basic value (See Van Oorschot Fig. 4  
6 “private key decryption” and “B’s high trust private key” and Col. 4 Lines 53-54); processing  
7 the unencrypted second section of said payload data stream using the processing method used  
8 when encrypting to deduce information characterizing the unencrypted second (See Van  
9 Oorschot Fig. 4 “X-fields” and Col. 6 Lines 45-47); linking said information and said basic value  
10 using the corresponding linkage as it has been used when encrypting to obtain said payload data  
11 key (See Van Oorschot Fig. 4 “Unlevelling” and “X-fields” and Col. 4 Lines 54-56); and  
12 decrypting the first section containing the encrypted payload data using said payload data key  
13 and said payload data encryption algorithm used when encrypting (See Van Oorschot Fig. 4  
14 “symmetric decryption” and “message”), but Van Oorschot failed to disclose that the second  
15 section included audio data, video data, a combination of audio data and video data, text data, or  
16 binary data forming an executable program.

17 Nardone teaches that movie data needs to be protected from being copied and that this is  
18 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further  
19 that in order to save on processing cost, only portions of the movie data should be encrypted (See  
20 Nardone Col. 1 Summary of the Invention).

21 It would have been obvious to the ordinary person skilled in the art at the time of  
22 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by

1 encrypting video data, and further by only encrypting portions of the data. This would have been  
2 obvious because the ordinary person skilled in the art would have been motivated to protect  
3 movie data and to save on processing cost.

4       Regarding claim 28, Van Oorschot disclosed a device for producing a payload data  
5 stream comprising a header and a payload data block containing encrypted payload data (See  
6 Van Oorschot Fig. 3 X-fields, header fields, and encrypted message field), comprising: a  
7 generator for generating a payload data key for a payload data encryption algorithm for  
8 encrypting payload data (See Van Oorschot Col. 6 Lines 41-43 and Fig. 3 “Create low trust  
9 symmetric key” K’); a first encryptor for encrypting a first section of the payload data using said  
10 payload data key and said payload data encryption algorithm to obtain an encrypted section of  
11 said payload data block of said payload data stream (See Van Oorschot Col. 6 Lines 42-43 and  
12 Fig. 3 “Symmetric encryption” and “encrypted message”), said first section including audio data,  
13 video data, a combination of audio data and video data, text data, or binary data forming an  
14 executable program (See Van Oorschot Abstract ciphertext), wherein a second section of the  
15 payload data remains unencrypted (See Van Oorschot Col. 6 Lines 45-47 “public key of entity  
16 A”); a processor for processing the unencrypted section of said payload data (See Van Oorschot  
17 Col. 6 Lines 45-50 “hash of X” which contains the public key of A) to deduce information  
18 characterizing the unencrypted second section of said payload data (See Van Oorschot Col. 6  
19 Lines 49-60  $h_{40}(X)$ ); a linker for linking said information and said payload data key by means of  
20 an invertible logic linkage to obtain a basic value (See Van Oorschot Col. 6 Lines 56-60 “K’  
21 XOR  $h_{40}(X)$ ”); a second encryptor for encrypting said basic value using a key of two keys being  
22 different from each other by an asymmetrical encryption method, said two different keys being

1 the public and the private keys respectively for said asymmetrical encryption method, to obtain  
2 an output value being an encrypted version of said payload data key (See Van Oorschot Col. 6  
3 Line 60 – Col. 7 Line 7); and entering said output value into said header of said payload data  
4 stream (See Van Oorschot Col. 6 Line 65 – Col. 7 Line 7 and Fig. 3 “A’s header field” and “B’s  
5 header field”), but Van Oorschot failed to disclose that the second section included audio data,  
6 video data, a combination of audio data and video data, text data, or binary data forming an  
7 executable program.

8 Nardone teaches that movie data needs to be protected from being copied and that this is  
9 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further  
10 that in order to save on processing cost, only portions of the movie data should be encrypted (See  
11 Nardone Col. 1 Summary of the Invention).

12 It would have been obvious to the ordinary person skilled in the art at the time of  
13 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by  
14 encrypting video data, and further by only encrypting portions of the data. This would have been  
15 obvious because the ordinary person skilled in the art would have been motivated to protect  
16 movie data and to save on processing cost.

17 Regarding claim 29, Van Oorschot disclosed a device for decrypting an encrypted  
18 payload data stream comprising a header and a payload data block containing a first section  
19 having encrypted payload data (encrypted message), said first section including audio data,  
20 video data, a combination of audio data and video data, text data, or binary data forming an  
21 executable program (See Van Oorschot Abstract ciphertext), and a second section having  
22 unencrypted payload data (public key of A), said header comprising an output value having been



1 generated by an encryption of a basic value by an asymmetrical encryption method using a key  
2 of two different keys including a private and a public key, said basic value representing a linkage  
3 of a payload data key, with which said first section having encrypted payload data is encrypted  
4 using a payload data encryption algorithm, and information deduced by a certain processing of  
5 the unencrypted second section of the payload data, said information characterizing a certain part  
6 of said payload data stream unambiguously (See rejection of claim 1 above), said device further  
7 comprising: means for obtaining said output value from said header (See Van Oorschot Fig. 4  
8 "B's Header Field" and Col. 4 Lines 51-52); a first decryptor for decrypting said output value  
9 using the other key of said asymmetrical encryption method to obtain said basic value (See Van  
10 Oorschot Fig. 4 "private key decryption" and "B's high trust private key" and Col. 4 Lines 53-  
11 54); a processor for processing the unencrypted second section of said payload data stream using  
12 the processing method used when encrypting to deduce information characterizing the  
13 unencrypted second (See Van Oorschot Fig. 4 "X-fields" and Col. 6 Lines 45-47); a linker for  
14 linking said information and said basic value using the corresponding linkage as it has been used  
15 when encrypting to obtain said payload data key (See Van Oorschot Fig. 4 "Unlevelling" and  
16 "X-fields" and Col. 4 Lines 54-56); and a second decryptor decrypting the first section  
17 containing the encrypted payload data using said payload data key and said payload data  
18 encryption algorithm used when encrypting (See Van Oorschot Fig. 4 "symmetric decryption"  
19 and "message"), but Van Oorschot failed to disclose that the second section included audio data,  
20 video data, a combination of audio data and video data, text data, or binary data forming an  
21 executable program.

1 Nardone teaches that movie data needs to be protected from being copied and that this is  
2 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further  
3 that in order to save on processing cost, only portions of the movie data should be encrypted (See  
4 Nardone Col. 1 Summary of the Invention).

5 It would have been obvious to the ordinary person skilled in the art at the time of  
6 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by  
7 encrypting video data, and further by only encrypting portions of the data. This would have been  
8 obvious because the ordinary person skilled in the art would have been motivated to protect  
9 movie data and to save on processing cost.

10 Regarding claim 2, Van Oorschot and Nardone disclosed that said payload data  
11 encryption algorithm is a symmetrical encryption algorithm (See Van Oorschot Fig. 3  
12 “symmetric encryption”).

13 Regarding claim 3, Van Oorschot and Nardone disclosed that said invertible logic linkage  
14 is self-inverting and includes an XOR- linkage (See Van Oorschot Col. 6 Lines 56-60).

15 Regarding claim 4, Van Oorschot and Nardone disclosed that one key of said two keys  
16 being different from each other is the private key of a producer of said payload data stream or the  
17 public key of a consumer of said payload data stream (See Van Oorschot Fig. 3 B’s high trust  
18 public key).

19 Regarding claim 5, Van Oorschot and Nardone disclosed that said part of said payload  
20 data stream being processed to deduce said information includes at least a part of said header  
21 (See Van Oorschot Fig. 3 “X-Field” and Col. 6 Lines 49-55).

1           Regarding claim 6, Van Oorschot and Nardone disclosed that said step of processing  
2 comprises forming a hash sum (See Van Oorschot Col. 6 Lines 49-55).

3           Regarding claim 7, Van Oorschot and Nardone disclosed further comprising the  
4 following step: identifying an algorithm being used in said step of processing by an entry into  
5 said header (See Van Oorschot Abstract Lines 14-16).

6           Regarding claim 14, Van Oorschot and Nardone disclosed that said step of processing  
7 further comprises the following sub-step: setting said entry for said output value in said header to  
8 a defined value and processing said entire header, including said entry set to a defined value (See  
9 Van Oorschot Fig. 3 “X-Field” and Col. 6 Lines 49-55).

10          Regarding Claim 16, Van Oorschot and Nardone disclosed the following step: identifying  
11 said payload data encryption algorithm by an entry into said header of said payload data stream  
12 (See Van Oorschot Abstract Lines 14-16).

13          Regarding claim 19, Van Oorschot and Nardone disclosed that said part being processed  
14 to deduce said information is said header (See Van Oorschot Fig. 4 “X-Fields”).

15          Regarding claim 23, Van Oorschot and Nardone disclosed that one key having been used  
16 when encrypting is the public key of said asymmetrical encryption method, while the other key  
17 having been used when decrypting is the private key of said asymmetrical encryption method  
18 (See Van Oorschot Fig. 3 “B’s high trust public key” and Fig 4 “B’s high trust private key”).

19          Regarding claim 24, Van Oorschot and Nardone disclosed that said step of processing  
20 includes forming a hash sum (See Van Oorschot Col. 6 Lines 49-55 and Fig. 4 “Unlevelling”).

21          Regarding claim 25, Van Oorschot and Nardone disclosed that a part of said header  
22 having been set to a defined value for said step of processing when encrypting is set to the same

1 defined value for said step of processing when decrypting (See Van Oorschot Fig. 3 “X-fields”  
2 and Fig. 4 “X-fields” wherein they must be the same defined value because they were both set by  
3 the sender upon sending).

4 Regarding claim 26, Van Oorschot and Nardone disclosed that said part of said header  
5 being set to a defined value includes said entry for said output value of said header (See Van  
6 Oorschot Fig. 3 “B’s header field” and Fig. 4 “B’s header field” wherein they must be the same  
7 defined value because they were both set by the sender upon sending).

8 Regarding claim 27, Van Oorschot and Nardone disclosed that said step of linking  
9 comprises using an XOR-linkage (See Van Oorschot Col. 6 Lines 56-60 and Col. 4 Lines 54-56  
10 and Fig. 4 “Unlevelling”).

11  
12 Claims 8, 11-12, 18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable  
13 over Van Oorschot and Nardone as applied to claims 1 and 17 above, and further in view of  
14 Matyas et al. (US Patent Number 5,200,999) hereinafter referred to as Matyas.

15 Van Oorschot and Nardone disclosed a system for sending a message from a sender to a  
16 receiver in which the message was encrypted using a key, the key was encrypted, and then the  
17 key was sent to the receiver with the encrypted message (See Van Oorschot Abstract and Fig. 3).  
18 Van Oorschot further disclosed decrypting the key, and using the key to decrypt the message at  
19 the receiver (See Van Oorschot Abstract and Fig. 4). However, Van Oorschot failed to disclose  
20 sending license data along with the key and message.

21 Matyas teaches that when sending a key, in order to authenticate the use of the key, and  
22 the validity of the key, certain data (License data) should be placed in the header along with the  
23 key. This data includes key type, key usage data (for history purposes), algorithm identifier,  
24 algorithm-specific data, key start date/time, key expiration data/time, device identifier, user  
25 identifier, key identifier, logical device identifier, and user-defined data (See Matyas Col. 13

1 Line 66 – Col. 14 Lines 60). Matyas further teaches that this information should be verified  
2 prior to use of the key (See Matyas Col. 100).

3 It would have been obvious to the ordinary person skilled in the art at the time of  
4 invention to employ the teachings of Matyas in the key and message sending system and method  
5 of Van Oorschot and Nardone by placing the license information, taught by Matyas, in the  
6 header of the message and checking this information prior to allowing the key and message to be  
7 decrypted. This would have been obvious because the ordinary person skilled in the art would  
8 have been motivated to protect the interests of the sender of the message and to ensure the  
9 security of the message.  
10

11 Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of  
12 Van Oorschot and Nardone and Matyas as applied to claim 8 above, and further in view of  
13 Klemba et al. (US Patent Number 5,710,814) hereinafter referred to as Klemba.

14 Van Oorschot and Nardone and Matyas disclosed sending license data for controlling the  
15 usage of a key and message, including usage history (See rejection of claim 8 above), but failed  
16 to disclose the data including how often the message could be decrypted.

17 Klemba teaches that license data can be used to control the number of uses of a  
18 cryptographic function (See Klemba Col. 14 Lines 14-19).

19 It would have been obvious to the ordinary person skilled in the art at the time of  
20 invention to employ the teachings of Klemba in the messaging system and method of Van  
21 Oorschot and Nardone and Matyas by using the license information to limit the number of times  
22 the message could be decrypted. This would have been obvious because the ordinary person  
23 skilled in the art would have been motivated to protect the interests of the sender of the message  
24 as well as to protect the message against compromise.  
25

1           Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination  
2   of Van Oorschot and Nardone and Matyas as applied to claim 8 above, and further in view of  
3   Edenson et al. (Us Patent Number 6,198,875) hereinafter referred to as Edenson.

4           Van Oorschot and Nardone and Matyas disclosed sending license data for controlling the  
5   usage of a key and message, including usage history (See rejection of claim 8 above), but failed  
6   to disclose the data including how often the message could be copied and how often it had  
7   already been copied.

8           Edenson teaches that license information can include how many copies of licensed data  
9   can be made (See Edenson Col. 4 Paragraph 2).

10          It would have been obvious to the ordinary person skilled in the art at the time of  
11   invention to employ the teachings of Edenson in the messaging system of Van Oorschot and  
12   Nardone and Matyas by including information regarding the number of allowed copies of the  
13   message that are permitted. This would have been obvious because the ordinary person skilled  
14   in the art would have been motivated to protect the interests of the message sender, and to protect  
15   the message itself from unauthorized distribution. Further, it would have been necessary to also  
16   keep track of the number of copies already made in order to enforce the copy limit.

17  
18          Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination  
19   of Van Oorschot and Nardone and Matyas as applied to claim 8 above, and further in view of  
20   Schneier ("Applied Cryptography Second Edition").

1           Van Oorschot and Nardone and Matyas disclosed sending license data for controlling the  
2           usage of a key and message, including usage history (See rejection of claim 8 above), but failed  
3           to disclose including the license in the hash function.

4           Schneier teaches that hashes are used to authenticate the data being hashed upon receipt  
5           of the data in order to detect any unauthorized changes to the data (See Schneier Pages 30-31  
6           Section 2.4).

7           It would have been obvious to the ordinary person skilled in the art at the time of  
8           invention to employ the teachings of Schneier in the messaging system of Van Oorschot and  
9           Nardone and Matyas by hashing the License data along with the X-fields. This would have been  
10          obvious because the ordinary person skilled in the art would have been motivated to protect  
11          against undetected changes to the license data sent with the message.

12  
13          Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot  
14          and Nardone as applied to claim 1 above, and further in view of Roediger (US Patent Number  
15          4,899,333).

16          Van Oorschot and Nardone disclosed sending a message from a sender to a receiver,  
17          including a header and a hash of the header (See Van Oorschot Col. 6), but Van Oorschot failed  
18          to disclose including a sender identifier and a receiver identifier in the header, or in the hash.

19          Roediger teaches that packet headers contain a source address (sender identifier) and a  
20          destination address (recipient identifier) and that a checksum should include these fields in order  
21          to ensure that the fields are not corrupted (See Roediger Col. 37 Lines 53-63).

1           It would have been obvious to the ordinary person skilled in the art at the time of  
2 invention to employ the teachings of Roediger in the messaging system of Van Oorschot and  
3 Nardone by including source and destination addresses in the header and including these in the  
4 hash. This would have been obvious because the ordinary person skilled in the art would have  
5 been motivated to provide means for routing the message from the sender to the receiver and  
6 allowing the receiver to verify that it was the intended receiver of the message.

7  
8           Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot  
9 and Nardone as applied to claim 17 above, and further in view of Schneier.

10          Van Oorschot and Nardone disclosed using a public key of the receiver for encryption  
11 (See rejection of claim 23 above) but failed to disclose using a private key of an asymmetrical  
12 key pair for encryption.

13          Schneier teaches that by encrypting data using a senders private key, the receiver can use  
14 the senders public key to authenticate the sender of the data (See Schneier Pages 53-54).

15          It would have been obvious to employ the teachings of Schneier in the messaging system  
16 of Van Oorschot and Nardone by encrypting the leveled key with the private key of the sender  
17 and decrypting it with the public key of the sender. This would have been obvious because the  
18 ordinary person skilled in the art would have been motivated to provide sender authentication at  
19 the receiver.

20



Art Unit: 2131

1 Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot  
2 and Nardone as applied to claims 28 and 29 above, and further in view of Kane et al. (US Patent  
3 Number 5,315,635) hereinafter referred to as Kane.

4 Van Oorschot and Nardone disclosed sending messages from a sender to a receiver (See  
5 Van Oorschot Abstract), but failed to disclose the sending being from a personal computer to a  
6 personal computer.

7 Kane teaches that messages can be sent between personal computers (See Kane Col. 1  
8 Lines 45-51).

9 It would have been obvious to the ordinary person skilled in the art at the time of  
10 invention to employ the teachings of Kane in the messaging system of Van Oorschot and  
11 Nardone by sending the encrypted messages from a sending personal computer to receiving  
12 personal computer. This would have been obvious because the ordinary person skilled in the art  
13 would have been motivated to protect messages sent between two personal computers.

#### 14 *Conclusion*


15 Claims 1-30 have been rejected and claim 31 has been cancelled.

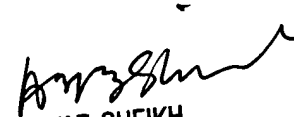
16 Any inquiry concerning this communication or earlier communications from the  
17 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.  
18 The examiner can normally be reached on M-F 8-4.

19 If attempts to reach the examiner by telephone are unsuccessful, the examiner's  
20 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the  
21 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent  
2 Application Information Retrieval (PAIR) system. Status information for published applications  
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished  
4 applications is available through Private PAIR only. For more information about the PAIR  
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR  
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would  
7 like assistance from a USPTO Customer Service Representative or access to the automated  
8 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

9  
10  
11   
12 Matthew Henning  
13 Assistant Examiner  
14 Art Unit 2131  
15 5/24/2006  
16

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100